

REMARKS

Claims 1 – 17 are presented for Examination. In the Office Action mailed on May 12, 2004, the Examiner rejected Claims 1 and 5 under 35 U.S.C. §102(b) as being anticipated by Dean et al. (U.S. Patent No. 6,173,173 B1); Claims 8 – 13, 15 and 17 under 35 U.S.C. §102(b) as being anticipated by Reeds, III et al. (U.S. Patent No. 5,204,902); Claim 2 under 35 U.S.C. §103(a) as being unpatentable over Dean in view of Applied Cryptography (hereinafter Schneier); Claims 3, 4, 6, and 7 under 35 U.S.C. §103(a) as being unpatentable over Dean in view of Deindl et al. (U.S. Patent No. 6,076,162); and Claims 14 and 16 under 35 U.S.C. §103(a) as being unpatentable over Reeds in view of Schneier. The Applicants respectfully traverse the Examiner's rejections.

35 U.S.C. §102(b): Claims 1 and 5

The Examiner states that Dean discloses all of the features of the instant claims. The Applicants respectfully submit that Dean teaches a system for tearing down a suspect call by an invalid mobile telephone. According to Dean, there are telephone systems that are not capable of tearing down suspect calls.

"Some of those techniques cannot directly interface with the MSC to terminate a 'suspected' call. For example, even if an RF fingerprint detection system detects a clone, the call is still established. There is no capability to block a call origination." Dean, col. 1, lines 22 – 26.

Dean solves part of this problem by using an authentication process, wherein a server sends a random key to an authorized client. Only the authorized clients are able to kill calls. The client uses the challenge, along with the shared secret text password that is stored at the client, to create a signature. The client signature is formed by appending the shared secret password to the random key.

"The client uses the challenge, along with the shared secret text password that is stored in the keys file on the OMP, to create a signature." Dean, col. 15, line 55 – col. 16, line 26.

Note that the "authorized client" in Dean is a vendor computer, not a subscriber identification module within a mobile communications unit. The vendor computer is being authenticated to *ensure that it is authorized to kill calls*.

In contrast, the instant claims are NOT directed to a system wherein a *shared* secret password is merely appended to a random key for authentication. The instant claims are directed to a system where the random key (a received challenge) is used to *generate* a set of additional keys, at least one kept at the locale of a subscriber identification module (SIM) and another that is sent to the communications unit. At the separate locations, each key is used to generate different signals (separately generated at each location) which are then brought together at the SIM to form a new signal (i.e., input value). The new signal is subsequently hashed at the SIM to form an authentication signal that is transmitted to the communications system. The goal of this complex processing is to *avoid passing a secret password* from the SIM to the communications unit housing the SIM. Note that the stated purpose of this Application is to thwart rogue communication units that may be programmed to steal passwords stored in the SIM. Hence, there are three entities involved in this authentication process, one of which is not a trusted party: the SIM, the communications unit, and the communications system. Dean teaches the authentication of *servers* within a communications system. Each authentication process is between just the server and the system: two entities.

The Examiner states that "Dean teaches random key generator that is capable of generating a plurality of keys, in response to a received challenge, if there was a plurality of subscribers." The Applicants respectfully disputes this assertion. The Applicants respectfully submit that a "challenge" is a term of art used within a challenge/response authentication system, wherein a challenge necessitates the need for a correct response that matches an expected response held by the challenger. The match is for the purpose of authenticating the respondee. Subscribers do not authenticate the system; the system authenticates subscribers. Logically, there is no need on the part of the subscriber to authenticate the system. Moreover, the instant claims are for generating a plurality of keys in response to a single received challenge, not a plurality of challenges.

The Examiner states that the digital signature taught by Dean is equivalent to an initial value taught by the claims. If this is assumed to be true, then the Examiner does not address the rest of the features in the claims, wherein the initial value is concatenated with a received signal to form an input value, which is then hashed to form an authentication signal. Nor does the Examiner address the received signal as being generated from a second key from the plurality of

keys, the second key being generated in response to the original, single received challenge. None of these features are taught by Dean after the formation of the digital signature.

However, if the Examiner's assertion is not true, i.e., the digital signature taught by Dean is equivalent to the authentication signal in the instant claims, then the instant claims teach additional features that are again not taught by Dean. Dean teaches the generation of a signature directly from the challenge and the shared secret text password. Dean does not teach the generation of any intermediate values that are used to generate the signature.

For the reasons stated above, the Applicants respectfully submit that Dean does not anticipate the instant claims.

35 U.S.C. §102(b): Claims 8 – 13, 15, and 17

The Examiner states that Reed discloses all of the elements of the instant claims. The Applicants respectfully disagree. Reed addresses the need to authenticate a mobile unit to the system. Reed does not address the need to circumvent rogue mobile units that are programmed to steal personal information from a subscriber identification module (SIM). Hence, Reed does not teach the use of SIMs, which is the subject matter of the instant claims. The Examiner states that Reed teaches SIMs at Col. 4, lines 27 – 31, but the Applicants were unable to find SIMs at the cited location. The cited location teaches:

"Each mobile unit has an electronic serial number (ESN) that is unique to that unit. The ESN number is installed in the unit by the manufacturer, at the time the unit is built (for example, in a read-only-memory), and it is unalterable."

The Applicants respectfully submit that a SIM is not an electronic serial number. An electronic serial number is a number which is unique to the mobile unit, not to the subscriber. It comprises data. As described in the instant Application, a SIM is a physical device that may be inserted into a mobile phone so that a subscriber may be appropriately billed when using different mobile phones. Hence, the subscriber and the mobile unit are different entities.

The Applicants respectfully submit that Reed teaches a mobile unit that maintains a shared secret data with the home system and uses the shared secret data to generate a signature. The instant claims are directed to a SIM that does NOT share secret data with the mobile unit, but uses information from the mobile to generate a signature that is later used by the mobile unit for authentication. This is directly contrary to the teachings in Reed, and so it is not taught by

Reed. Hence, the Applicants respectfully submit that the instant claims are not anticipated by Reed.

35 U.S.C. §103(a): Claim 2

The Applicants respectfully submit that the instant claim is dependent upon a patentable independent claim. Hence, the Applicants respectfully submit that the instant claim also incorporates features that are not taught by the cited references.

35 U.S.C. §103(a): Claims 3, 4, 6, and 7

The Applicants respectfully submit that the instant claims are dependent upon a patentable independent claim. Hence, the Applicants respectfully submit that the instant claims also incorporate features that are not taught by the cited references.

35 U.S.C. §103(a): Claims 14 and 16

The Applicants respectfully submit that the instant claims are dependent upon a patentable independent claim. Hence, the Applicants respectfully submit that the instant claims also incorporate features that are not taught by the cited references.

CONCLUSION

In light of the arguments presented above, the Applicants respectfully submit that the instant claims are patentable. Accordingly, reconsideration and allowance of this Application is earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: November 10, 2004

By: 

Kyong H. Macek
Reg. No. 42,977
Attorney for the Applicants

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 651-5797
Facsimile: (858) 658-2502